UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,320	12/12/2003	Robert Joseph Harley	Harley-004	9086

7590 07/26/2007

Mr. Robert J. Harley
4, rue de l'Ermitage
Sevres, 92310
FRANCE

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,320	HARLEY, ROBERT JOSEPH	
	Examiner	Art Unit	
	Carlton V. Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed on **12-12-2003**.

2. Claims **1 - 9** are pending. Claim **1** is independent.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims **1 - 9** are rejected under 35 U.S.C. 101 because the claimed invention is based on non-statutory subject matter and directed towards nothing more than the abstract idea of a mathematical algorithm. Abstract ideas are not eligible for patent protection. A claimed invention reciting a computer program product that solely calculates a mathematical formula or a computer readable medium that solely stores a mathematical formula is not directed to the type of subject matter eligible for patent protection. Claims **1 - 9** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims **1 - 9** are so broad as to cover each and every practical application. Claims **1 - 9** do not produce a tangible result. Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 103 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -
(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claim **1 - 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hoffstein et al.** (US Patent No. **7,031,468**) in view of **Gressel et al.** (US Patent No. **6,748,410**) and further in view of Penner (US Patent No. **7,158,569**).

Each independent section of the claimed invention will be addressed. The independent claim and the dependent claims based upon that independent claim recite instructions utilized to perform mathematical computations, procedures, or steps, such as multiplication and addition (i.e. summing), for an algorithm utilizing computer system processor(s) and system register(s).

Regarding Claims 1 - 9, Hoffstein-Gressel-Penner disclose a method for computing the number of points on an elliptic curve over a finite field, in which a Frobenius equation is solved to a given precision by first and second parts, wherein said parts comprise the following steps:

a) Said first part firstly computes a first partial solution of said equation using said first part recursively to reduced precision, b) Said first part secondly applies a Frobenius operation to said first partial solution, c) Said first part thirdly computes an error term for said equation, d) Said first part fourthly computes correction factors for said equation, e)

Said first part fifthly computes a second partial solution using said second part to reduced precision, f) Said first part sixthly combines said first partial solution and said second partial solution, g) Said second part firstly computes a first partial solution of said equation using said second part recursively to reduced precision, h) Said second part secondly applies a Frobenius operation to said first partial solution, i) Said second part thirdly updates said error term, j) Said second part fourthly computes a second partial solution using said second part recursively to reduced precision, k) Said second part fifthly combines said first partial solution and said second partial solution.

Claims 2 - 9 disclose precision operations, Teichmuller type operations, finite-field operations, canonical lift, multiplicative operations, p-adic number operations (groupings of numbers along an elliptic curve), manipulation of elliptic curve algorithms, and generation key.

Hoffstein discloses:

(see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves; col. 4, lines 20-22: multiplicative operations; col. 3, lines 54-56: finite field polynomial operations; col. 1, lines 56-59: p-adic numbers (computing the number of points on elliptic curves over a finite field); col. 2, lines 18-25: cryptographic key generation))

Hoffstein does not specifically disclose the following limitations.

However, Gressel discloses:

(see Gressel col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations; col. 3, lines 28-32: cryptographic key generation)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein as taught by Gressel to enable the capability to perform partial algorithmic operations. One of ordinary skill in the art would have been motivated to employ the teachings of Penner in order to enable the capability to provide for accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45: " ... *The present invention seeks to provide improved apparatus and methods for modular multiplication and exponentiation and for serial integer division, and for accelerating and securing modular arithmetic processors and accelerating memory transfers to computer peripheral that need simplified accelerated memory to peripheral data transfers with limited CPU core changes.* ... ")

Hoffstein-Gressel does not specifically disclose the following limitations.

However, Penner discloses:

(see Penner col. 7, lines 25-29; col. 25, lines 13-17: canonical lift; col. 26, line 31: Teichmuller lift of a given finite-field polynomial; col. 19, lines 29-33; col. 20, lines 11-16: recursive operations; col. 20, lines 8-11: error terminate; col. 1, lines 62-63: precision algorithmic operations)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein as taught by Penner to enable the capability to perform canonical, Teichmuller, recursive, and error type algorithmic operations. One of ordinary skill in the art would have been motivated to employ the teachings of Penner in order to enable the capability to provide new, novel, and efficient methods for calculating algorithmic transform operations. (see Penner col. 1, lines 52-55: " ... *In combination with these wavelet filters, the invention also provides new methods for calculating various classical transforms including the Fourier transform and its inverse. This immediately provides novel and efficient methods for digital filtering. ...* ")

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7/22/07

CVJ
July 9, 2007